Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 2 (2010) 143–148

Procedia Computer Science

www.elsevier.com/locate/procedia

ICEBT 2010

Tamperproof Transmission of Fingerprints Using Visual Cryptography Schemes

Thomas Monoth* , Babu Anto P

[a]*Department of Information Technology, Kannur University, Kerala -670567, India*

Abstract

Visual Cryptography and biometrics have been identified as the two most important aspects of digital security. In this paper, we propose a method for the preparation and secure transmission of fingerprint images using visual cryptography scheme. Visual cryptography (VC) is a kind of secret image sharing scheme that uses the human visual system to perform the decryption computations. A visual cryptography scheme (VCS) allows confidential messages to be encrypted into *k-out-of-n* secret sharing schemes. Whenever the number of participants from the group (n) is larger than or equal to the predetermined threshold value (k), the confidential message can be obtained by these participants. VCS is interesting because decryption can be done with no prior knowledge of cryptography and can be performed without any cryptographic computations. In this paper, the fingerprint image is broken up into n pieces, which individually yield no information about the image. These pieces of the images, called shares or shadows, may then be distributed among a group of n participants/dealers. By combining any k ($k \leq n$) of these shares, the original fingerprint image can be recovered, but combining less than k of them will not reveal any information about the image. The scheme is perfectly secure and very easy to implement. To decode the encrypted information, i.e., to get the original information back, the shares are stacked and the secret image pops out. The only drawback of the VCS is the loss in contrast of reconstructed image. The proposed method for the reconstruction of fingerprint image is based on XNOR operation. This will enable one to obtain back perfect fingerprint image.

Keywords: visual cryptography; visual secret sharing; biometric image; fingerprints.

1. Introduction

The increasing dependence on computers at all levels of our life, personal and sensitive information is increasingly being stored and transmitted using computer systems and networks everyday. This revolution, however, has brought with it new threats and computer crimes as noticed in the increased number of computer attacks and break-ins. Replicating important information will give greater chance to intruders to access it. On the other hand, having only one copy of this information means that if this copy is destroyed there is no way to retrieve it. Thus, there is a great need to handle information in a secure and reliable way. In such situations, secret sharing is of great relevance. The basic idea of secret sharing is to divide the information into pieces, so that qualified subsets of these pieces (shares) can be used to recover the secret. Intruders need to get access to several shares to retrieve the information. Similarly, they need to destroy several shares to destroy the information.

The concept of secret sharing was independently introduced by Blakley [1] and Shamir [2] in 1979. Secret sharing becomes indispensable whenever secret information needs to be kept collectively by a group of participants in such a way that only a qualified subgroup is able to reconstruct the secret. An example of such a scheme is a *k-out-of-n* threshold secret sharing in which there are n participants holding their shares of the secret and every k ($k \leq n$) participants can collectively recreate the secret while any $k-1$ participants cannot get any information about the secret. The need for secret sharing arises if the storage system is not reliable and secure. Secret sharing is also useful if the owner of the secret does not trust any single person [3]. This concept

* Corresponding author. Tel.:+919447283326; fax: +914935241087
E-mail address: isres@yahoo.com.

1877-0509
doi:10.1016/j.procs.2010.11.018

was first applied to numbers, but in the 1990s, researchers extended it to images. Visual cryptography implements secret sharing for images [4].

The biometrics technology brings a new dimension to individual identity verification. It provides a guaranteed level of accuracy and consistency over traditional methods. Biometrics means "the statistical analysis of biological observations and phenomena". It refers to the use of distinctive physical (e.g., fingerprints, face, retina, iris, hand geometry, palm) and behavioural (e.g., gait, signature, speech) characteristics for automatically recognizing individuals [5].

2. Biometrics systems

Biometric characteristics provide a unique natural signature of a person and it is widely accepted. Each biometric technique has its advantages and disadvantages. The applicability of a specific biometric technique depends heavily on the application domain. No single biometric can meet the entire requirement (e.g. accuracy, cost, practicality, etc.)[6]. Fingerprints have been used as a biometric characteristic because they could offer unique advantages over other biometrics in terms of acquisition ease, relative temporal invariance and uniqueness among different subjects. A brief comparison of biometric techniques based on five factors is provided in Table1. In this sense, each biometric technique is admissible. For example, it is well known that both the fingerprint technique and the iris scan technique perform much better than the voice print technique in terms of accuracy and speed. As can be seen from Table 1, overall fingerprints perform better than other biometric techniques [7]. A fingerprint has its own distinctiveness that has been used for personal identification for several years. Fingerprint identification is based on two basic premises:

- Persistence: the basic characteristics of fingerprints do not change with time.
- Individuality: everybody has a unique fingerprint.

Biometrics can operate in one of two modes: the identification mode, in which the identity of an unknown user is determined, and the verification mode, in which a claimed identity is either accepted or rejected. On this basis biometrics were applied in many high end applications, with governments, defence and airport security being major customers. However, there are some areas in which biometric applications are moving towards commercial application, namely, network/PC login security, web page security, employee recognition, time and attendance systems, and voting solutions. The biometric systems also enhance user convenience by alleviating the need to design and remember passwords.

Table 1. Comparison of various biometric technologies

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention	Average
Face	100	50	75	100	50	100	50	75.0
Fingerprint	75	100	100	75	100	75	100	89.3
Hand - geometry	75	75	75	100	75	75	75	78.6
Keystrokes	50	50	50	75	50	75	75	60.7
Hand veins	75	75	75	75	75	75	100	78.6
Iris	100	100	100	75	100	50	100	89.3
Retinal scan	100	100	75	50	100	50	100	82.1
Signature	50	50	50	100	50	100	50	64.3
Voice	75	50	50	75	50	100	50	64.3
Gait	75	50	50	100	50	100	75	71.4

3. Visual cryptography schemes

Visual cryptography, proposed by Naor and Shamir [4], is one of the cryptographic methods to share secret images. A visual cryptography (VC) for a set P of *n* participants is a method to encode a secret image (SI) into *n* shadow images called shares, where each participant in P receives one share. Certain qualified subsets of participants can visually recover the SI, but other, forbidden sets of participants have no information on the SI. A 'visual recovery' of the qualified set X means that they can see the SI by xeroxing the shares given to the participants in X onto transparencies and then stacking them. Thus, the participants in a qualified set X will be able to see the SI without any knowledge of cryptography and without performing any cryptographic computation.

The VCS describes the way in which an image is encrypted and decrypted. There are different types of visual cryptography schemes (VCS) [8-10]. For example, there is the *k-out-of-n* scheme that says *n* shares will be produced to encrypt an image, and *k* shares must be stacked to decrypt the image. If the number of shares stacked is less than *k,* the original image is not revealed. The other schemes are *2-out-of-n* and *n-out-of-n* VCS. In the *2-out-of-n* scheme *n* shares will be produced to encrypt an image, and any two shares must be stacked to decrypt the image. In the *n-out-of-n* scheme, *n* shares will be produced to encrypt an image, and *n* shares must be stacked to decrypt the image. If the number of shares stacked is less than *n,* the original image is not revealed. Increasing the number of shares or participants will automatically increase the level of security of the encrypted message.

3.1. The existing model

Let P = {1, 2,. . . , n} be a set of elements called participants and let 2^P denote the collection of all subsets of P. Let $\Gamma_Q \subseteq 2^P$ and $\Gamma_F \subseteq 2^P$, where $\Gamma_Q \cap \Gamma_F = \theta$ .The members of Γ_Q are called qualified sets and members of Γ_F are called forbidden sets. The pair (Γ_Q, Γ_F) is called the access structure of the scheme [8].

Define Γ_O which consist of all minimal qualified sets:

$$\Gamma_O = \{ A \in \Gamma_Q : A^{|} \notin \Gamma_Q \text{ for all } A^{|} \subset A \}$$

The message (secret data) consists of a collection of black and white pixels. Each pixel appears in n version called shares, one for each transparency. Each share is a collection of m black and white subpixels. The resulting structure can be described by an n x m Boolean matrix $S = [s_{ij}]$, where

$s_{ij} = 0 \iff$ the j^{th} subpixel in the i^{th} share is black.

$s_{ij} = 1 \iff$ the j^{th} subpixel in the i^{th} share is white.

Let (Γ_Q , Γ_F) be an access structure on a set of n participants. A $(\Gamma_Q , \Gamma_F, \alpha)$- VCS with the relative difference α and set of thresholds $1 \le d \le m$ is realized using the two n x m basis matrices S^0 and S^1 if the following two conditions hold:

(1). If $X = \{ i_1, i_2, \ldots\ldots i_p \} \in \Gamma_Q$, then the "or" V of rows $i_1, i_2, \ldots\ldots i_p$ of S^0 satisfies $H(V) \le d - \alpha .m$; whereas, for S^1 it results that $H(V) \ge d$.

(2). If $X = \{ i_1, i_2, \ldots\ldots i_p \} \in \Gamma_F$, then the two p x m matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots\ldots i_p$ are identical up to a column permutation.

The first condition is called contrast and the second condition is called security. The contrast should be as large as possible and at least one subpixel over the *m* subpixels, that is $\alpha \ge 1/m$. The second condition is called security; it implies that by inspecting the shares of nonqualified subsets of participants one cannot identify whether the shared pixel is white or black. The collections of matrices C_0 and C_1 are obtained by permuting the columns of the basis matrices S^0 and S^1 in all possible ways [9]. The important parameters of the scheme are:

- *m*, the number of subpixels in a share. This represents the loss in resolution from the original image to the shared one. The *m* should be as small as possible. The *m* is computed using the equation:

$$m = 2^{n-1} \quad (1)$$

- α, the relative difference. It determines how well the original image is recognizable. This represents the loss in contrast. The α should be as large as possible. The relative difference α is calculated using the equation:

$$\alpha = | n_b - n_w | / m \quad (2)$$

where n_b and n_w are the number of the black subpixels which are generated from a black and white pixels in the original image, respectively.

- β, the contrast. The value β is to be as large as possible. The minimum contrast that is required to ensure that the black and white areas will be distinguishable is $\beta \ge 1$. The contrast β is computed using the equation:

$$\beta = \alpha.m \quad (3)$$

3.2. Basic theory

The basic idea of visual cryptography can be best described by considering a *2-out-of-2* VCS. Let us consider a binary secret image S containing exactly *m* pixels. The dealer creates two shares (binary images), S_1 and S_2, consisting of exactly two pixels for each pixel in the secret image as shown in Table 1. If the pixel in S is black, the dealer randomly chooses one row from the first two rows of Table 1. Similarly, if the pixel in S is white, the dealer randomly chooses one row from the last two rows of Table 2.

Table 2. The pixel pattern for *2-out-of-2* VCS with 2-subpixels layout

Pixel color	Original Pixel	Share1	Share2	Share1+ Share2
Black	■	■□	□■	■■
Black	■	□■	■□	■■
White	□	■□	■□	■□
White	□	□■	□■	□■

To analyse the security of the *2-out-of-2* VCS, the dealer randomly chooses one of the two pixel patterns (black or white) from the Table1 for the shares S_1 and S_2. The pixel selection is random so that the shares S_1 and S_2 consist of equal number of black and white pixels. Therefore, by inspecting a single share, one cannot identify the secret pixel as black or white. Therefore, this method provides perfect security. The two participants can recover the secret pixel by superimposing the two shared

subpixels. If the superimposition results in two black subpixels, the original pixel was black; if the superimposition creates one black and one white subpixel, it indicates that the original pixel was white[4][9].

We mathematically represent the white pixel by 1 and the black pixel by 0. For the *2-out-of-2* VCS, the basis matrices, S^0 and S^1 are designed as follows:

$$S^0=\begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix} \qquad S^1=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

Using the equations (2) and (3) above, for the basis matrices the relative difference α and contrast β can be computed as:

$$\alpha = ½ \text{ and } \beta = 2 \qquad \text{(a)}$$

There are two collections of matrices, C_0 for encoding white pixels and C_1 for encoding black pixels. Let C_0 and C_1 be the following two collections of matrices:

$$C_0 = \{\text{Matrices obtained by permuting the columns of } \begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}\}$$

$$C_1 = \{\text{Matrices obtained by permuting the columns of } \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\}$$

That is,

$$C_0 = \{ \begin{bmatrix}1 & 0\\ 1 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\ 0 & 1\end{bmatrix}\} \text{ and } \quad C_1 = \{ \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\}$$

To share a white pixel, the dealer randomly selects one of the matrices in C_0, and to share a black pixel, the dealer randomly selects one of the matrices in C_1**.** The first row of the chosen matrix is used for share S_1 and the second for share S_2. For example, a row (0 1) defines the black-white scheme in a share. Throughout this paper, C_0 and C_1 will denote the collections of matrices used to randomly select a share scheme to encode a white or black pixel from the original image.

3.3. Example

The Figure 1 depicts example for *2-out-of-2* VCS with two subpixel layouts.

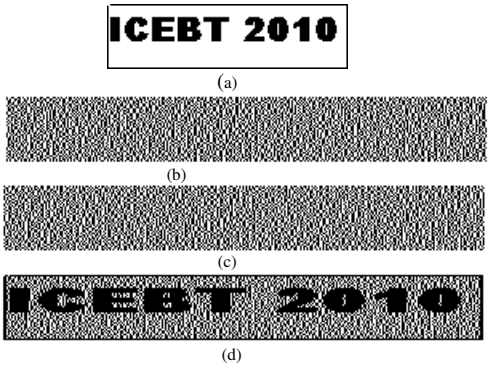

Fig.1. A *2-out-of-2* VCS with 2-subpixel layout: (a) the original image S;(b) the first share S_1, (c) the second share S_2;and (d) superimposed S_1 and S_2.

The problem that arises with this scheme is that for every pixel encoded from the original image into two subpixels and placed on each share in a horizontal or vertical fashion (here horizontal), the shares have a size of s x 2s if the secret image is of size s x s. Hence there is distortion.

To avoid the horizontal or vertical distortion of the reconstructed image, we can use the 4-subpixel layout [4].

In the 4-subpixel layout, the shares have a size of *2s x 2s* if the secret image is of the size *s x s*. Hence there is no horizontal or vertical distortion in the reconstructed image. The only change is that the image is *m* times larger than the original. There is uniform pixel expansion, but no distortion.

It is also possible to do VCS without enlargement of the reconstructed image. Now we explain the generation of shares with consistent share size using random basis column pixel expansion technique [10]. In this technique, the shares have a size *s x s* if the secret image is of the size *s x s*. That is, the reconstructed image is identical to the original image.

In this paper we proposed VCS model using random basis column pixel expansion technique.

4. Proposed method

In order to demonstrate that the proposed scheme is feasible, some experiments were conducted using *2-out-of-2* VCS. These are discussed in this section.

In the proposed method the biometric data (fingerprint image) is combined with visual cryptography. The resulting cipher will become very hard to break, because we use two different security techniques. The fingerprint image is called the ciphertext (C). Then we encrypt this ciphertext (C) into another ciphertext($C^{/}$) by using visual cryptography schemes. While encrypting, the ciphertext (C) is converted into share images. The ciphertext($C^{/}$) is collection of shares, which individually yield no information about the original image. For many ciphers, multiple encryptions does not strengthen the cipher, hence it is often waste of time, but in this case, it strengthens the cipher considerably. The proposed type of cryptosystem overcomes any type attacks.

The proposed method will have three phases:

Shares building phase: During this phase, a trusted entity, usually called the share-builder, is supplied with required input (here fingerprint image) to produce a share for each shareholder.

Shares distribution phase: In shares distribution phase, the shares produced in the first phase are delivered to the shareholders. Usually secure channels are used for communication between share-builder and shareholders.

Secret reconstruction phase: During secret reconstruction phase, a qualified subset of shareholders will pool their shares to a trusted entity, usually called secret-builder, to reconstruct the secret. Reconstructing the secret needs to be secure. All shares should be submitted to secret-builder over secure channels to insure privacy.

In this method fingerprint image is divided into a number of shares (S_1 to S_n) and stored in n different servers. Only the pre-specified subset of Si's (pre-specified servers) are eligible (qualified subset shares/servers) to retrieve the secret information. This will improve both availability and confidentiality. An adversary or hacker needs to steal a qualified subset of shares in order to be able to decode the secret information. The loss of some shares (because of server collapse, for example) is tolerated as long as a qualified subset of shares is still available. This will provides collaborative security.

5. Experimental result

The experiment described is based on a *2-out-of-2* VCS with 4-subpixel layout using random basis column pixel expansion technique.

In this experiment, the fingerprint considered for explication is a binary image in BMP format. To perform the encryption process we have created a program (using MATLAB) to encrypt fingerprint image files into two shares, so that the original image is visible only when we overlay the two shares using XNOR operations. The Figure 2 depicts the encryption and decryption processes of the fingerprint image using VCS based on XNOR operation.

Fig. 2(a).Original Image (Fingerprint Image).

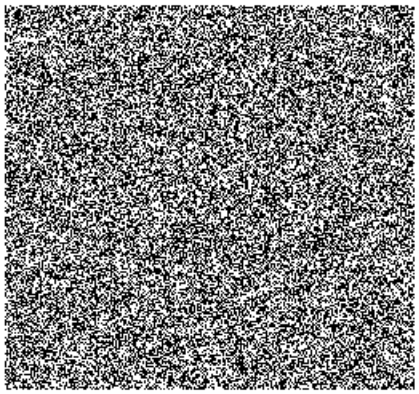

Fig. 2(b). Share 1

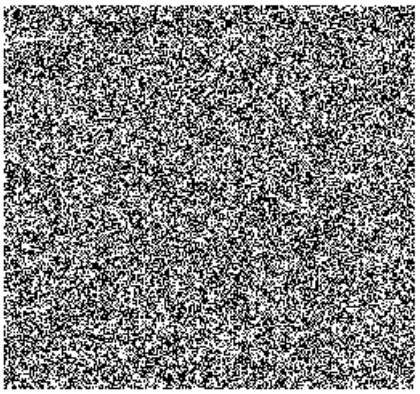

Fig. 2(c). Share 2.

Fig. 2d. Decrypted Fingerprint Image using XNOR Operation

This experiment can be easily expanded to *k-out-of-n* VCS. The scheme is perfectly secure and very easy to implement. To decode the encrypted information, i.e., to get the original information back, the shares are stacked and the fingerprint image pops out. The major advantage of this method is that decryption process (fingerprint reconstruction phase) could not required any complex algorithm and computations. The proposed method is less complex and fast compared to other cryptosystems.

6. Conclusions

This work shows, using a simple example, the application of *2-out- of-2* VCS. Different variations of this method are also possible. The work also leaves open the scope for future expansions which address emerging dependence on computers at all levels of applications. Fingerprint information is being stored and transmitted increasingly using computer systems and networks everyday. This revolution, however, has brought with it new threats and computer crimes as evidenced by the increasing number of computer attacks and break-ins. Therefore, there is a great need to keep information in a secure and reliable manner. Thus this work has direct application in individual identity verification and security requirements for e-documents, especially in the context of the ever-increasing applicability and relevance of online fingerprint transactions.

References

[1] G.R. Bakley, *Safeguarding Cryptographic Keys*, in Proc. AFIPS National Computer Conference, 48 (1979) 313-317.
[2] A. Shamir, *How to Share a Secret*, Communications of the ACM, 22(1979) 612-613.
[3] Josef Pieprzyk, Thomas Hardjono and Jennifer Sberry, *Fundamentals of Computer Security*, Springer (2003).
[4] M. Naor and A. Shamir, *Visual Cryptography*, Advances in Cryptology-Eurocrypt'94, LNCS 950: (1995)1-12.
[5] A. K. Jain and D. Maltoni, *Handbook of Fingerprint Recognition*: Springer- Verlag New York, Inc. (2003).
[6] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, *Biometric cryptosystems: issues and challenges*, *Proc. of the IEEE*, vol. 92 (2004) 948-960.
[7] A. Jain, L. Hong, and R. Bolle, *On-Line Fingerprint Verification*, IEEE Trans. Pattern Anal. Mach. Intell., vol. 19, (1997) 302-314.
[8] Daoshun Wang, FengYia, XiaoboLi, *On general construction for extended visual cryptography schemes,* Pattern Recognition: 42 (2009) 3071-3082.
[9] Borko Furht, Edin Muharemagic and Daniel Socek, *Multimedia Encryption and Watermarking*, Springer, (2005).
[10] Thomas Monoth & Babu Anto P. *Recursive Visual Cryptography Using Random Basis Column Pixel Expansion,* Proc. of the IEEE International Conference on Information Technology(ICIT '07), (2007), 41-43.